UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,430	06/27/2000	Guangyu Zhao	CISCO-2402	7891

7590 07/27/2004

Jonathan Velasco
Sierra Patent Group, Ltd.
P.O. Box 6149
Stateline, NV 89449

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	4

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/607,430	ZHAO ET AL.
	Examiner	Art Unit
	Kambiz Zand	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06/27/2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-27** have been examined.

Drawings

2. New formal drawings are required in this application because original drawings by the applicant were objected to by Examiner/the Draftsperson under 37 CFR 1.84 or 1.152. Please see attached PTO-948. Correction is requested.

Claim Objections

3. **Claims 7, 10-12, 14, 16-18, 20 and 22** are objected to because of the following informalities: typo error. Examiner suggests the following corrections:

Claim 7:

- Replacement of phrase "a" (line 2) with phrase "an".

Claims 10 and 22:

- Delete the phrase "the, first occurrence" line 3.
- Inserting phrase "incoming" after the phrase "the, second occurrence" (line 3).

Claims 11, 12, 17 and 18:

- Replacement of phrase "files" (line 2) with phrase "file".

Claims 14 and 20:

- Replacement of phrase "b" (line 4) with phrase "c".

Claim 16:

- Delete the phrase "the, first occurrence" (line 4).
- Inserting phrase "incoming" after the phrase "the, second occurrence" (line 4).
- Replace the phrase "the, third occurrence" with phrase "a" (line 4).
- Replace the phrase "the" with phrase "a" (line 5).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

5. **Claims 9** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. **Claims 9** recite the limitation "said document uploaded commands" in the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. **Claims 1-5, 10-13, 16-19 and 22-25** are rejected under 35 U.S.C. 102(b) as being anticipated by Chen et al (5,832,208 A).

- Examiner refers Applicant to col.6, lines 58-63 where "e-mail messages" is being used to describe all types of files, messages, broadcasts and communications used within, sent from or received by a mail server. Therefore Examiner considers any reference to e-mail messages corresponds to incoming files of Applicant's claims limitations. As an example" scanning of all e-mail messages corresponds to scanning of all incoming files.

- Col.5, lines 54-56 refer to centralized virus detection operations at the server level. Therefore Examiner considers any reference to e-mail server or other name server by Chen et al corresponds to "networked server" of Applicant's claim limitation.

- Col.6, lines 1-4 disclose that the system is capable of scanning all incoming files as they are received.

As per claim 1 Chen et al (5,832,208 A) teach in a networked server (**see fig.2, item 130 where the mail server corresponds to networked server**) having a file system therein (**see fig.2, item 140; col.7, lines 11-16 where the message system corresponds to applicant's file system**), a virus detection monitoring system (**see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus**) comprising:

a) a check-in interceptor configured to monitor the network server for incoming files and intercept incoming files before said files are transferred to the file system of the server (**see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed**) and

b) an anti-virus interface operatively coupled to said check-in interceptor (**see fig.2, item 110 where item 110 also corresponds to Applicant's anti-virus interface, that is the agent not only monitors the incoming files as an check in interceptor but it also act as an interface between the server and the antivirus application of 120;**

also see col.7, lines 48-56 where upon detection of attachment it send the file to anti virus application), said anti-virus interface configured to transfer the incoming files, which are intercepted, to an anti-virus application for virus detection and removal (**see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted**).

As per claim 2 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 1 wherein said anti-virus interface is further configured to receive from said anti-virus application a signal indicating whether a virus was detected in the intercepted incoming file and whether the virus was removed **(see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5)** .

As per claim 3 Chen et al (5,832,208 A) Chen et al teach the virus detection monitoring system of claim 1, wherein said check-in interceptor is further configured to prevent an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file (**see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-**

attachment to the file are being processed and that represent the act of prevention).

As per claim 4 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 1, wherein said check-in interceptor is further configured to prevent an intercepted incoming file from entering the file system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application **(see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repaired that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent)**.

As per claim 5 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 1 wherein said anti-virus interface is further configured to receive from said anti-virus application a signal indicating whether a virus was detected in the intercepted incoming file **(see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5)**, said check-in interceptor further configured to communicate the signal to a user submitting the intercepted incoming file **(see col.7, lines 60-65 where the alert may be transmitted to network**

node originated the infected attachment that corresponds to the user who submitted the virus in the first place).

As per claim 10 Chen et al (5,832,208 A) teach in a networked server(**see fig.2, item 130 where the mail server corresponds to networked server**) having a file system (**see fig.2, item 140; col.7, lines 11-16 where the message system corresponds to applicant's file system**) therein, a method for virus detection monitoring (**see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus)** comprising:

a) intercepting the incoming files before the files are transferred to the file system of the server (**see fig.2, item 110 where the agent intercepts and check all incoming files; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed**); and

b) transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal (**see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted**).

As per claim 11 Chen et al (5,832,208 A) teach the method of claim 10, further comprising preventing an intercepted incoming file from entering the files system if a

virus is detected in the intercepted incoming file **(see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the act of prevention**).

As per claim 12 Chen et al (5,832,208 A) teach the method of claim 10, further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application **(see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repair that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent)**.

As per claim 13 Chen et al (5,832,208 A) teach the method of claim 10, further comprising:

a) receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file (**see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the**

virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5); and

b) communicating the signal to a user submitting the intercepted incoming file **(see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place)**.

As per claim 16 Chen et al (5,832,208 A) teach a program storage device readable by a machine(**see fig.2, item 130 where the mail server corresponds to networked server that is a readable machine having storage device**), tangibly embodying a program of instructions executable by the machine to perform a method for virus detection monitoring (**see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus)**, said method comprising:

a) intercepting the incoming files before the files are transferred to the file system of the server (**see fig.2, item 110 where the agent check-in all incoming files; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed**); and

b) transferring the incoming files which are intercepted to an anti-virus

application for virus detection and removal (**see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted**).

As per claim 17 Chen et al (5,832,208 A) teach the program storage device of claim 16, said method further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file (**see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the act of prevention**).

As per claim 18 Chen et al (5,832,208 A) teach the program storage device of claim 16, said method further comprising preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application **(see col.8, lines 7-15 where if the attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repair that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent)**.

As per claim 19 Chen et al (5,832,208 A) teach the program storage device of claim 16, said method further comprising:

a) receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file (**see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5**); and

b) communicating the signal to a user submitting the intercepted incoming file **(see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place)**.

As per claim 22 Chen et al (5,832,208 A) teach in a networked server (**see fig.2, item 130 where the mail server corresponds to networked server**) having a file system (**see fig.2, item 140; col.7, lines 11-16 where the message system corresponds to applicant's file system**) therein, a virus detection monitoring system (**see abstract where detection and removal of virus application in combination with server network and peripheral devices and interfaces corresponds to Applicant's virus detection monitoring system that monitors incoming files for virus)** comprising:

a) means for intercepting the incoming files before the files are transferred to the file system of the server (**see fig.2, item 110 where the agent corresponds to check-in interceptor as means for intercepting all incoming files; col.7, lines 32-53 where**

the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed); and

b) means for transferring the incoming files which are intercepted to an anti-virus application for virus detection and removal (**see col.7, lines 48-67 where if virus detected then the infected attachment is being deleted and the means for transfer if the agent 110 of fig.2**).

As per claim 23 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising means for preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file (**see fig.2, item 110 where the agent corresponds to check-in interceptor; col.7, lines 32-53 where the agent 110 monitors files for any type of attachment and forward the files to item 120 for virus detection and removal, the files do not transferred to the file system until the process of checking and re-attachment to the file are being processed and that represent the means of prevention**).

As per claim 24 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising means for preventing an intercepted incoming file from entering the files system if a virus is detected in the intercepted incoming file and the virus was not removed by the anti-virus application (**see col.8, lines 7-15 where if the**

attachment or virus is not removed after the interception as outlined in claim 1 above, then attempt to cure the file being conducted and only in case of file repair that the agent may attachment may be re-attach to the file by the agent which means that if not cured or not removed the incoming file will not be forwarded by the agent).

As per claim 25 Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising:

a) means for receiving a signal from said anti-virus application, said signal indicating whether a virus was detected in the intercepted incoming file (**see col.7, lines 57-67 anti virus application send an alert indicating a detection of virus and delete the virus before being send a signal to the agent for scanning the next file as described in col.8, lines 1-5 as the means of detection of virus and alert as means of receiving the signal)**; and

b) means for communicating the signal to a user submitting the intercepted incoming file **(see col.7, lines 60-65 where the alert may be transmitted to network node originated the infected attachment that corresponds to the user who submitted the virus in the first place)**.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 6, 14, 20 and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (5,832,208 A) in view of Hodges et al (6, 269,456 B1).

As per claim 6 Chen et al (5,832,208 A) teach all limitation of the claim as applied to claim 1, above but do not explicitly disclose a "dat file updater and validater" coupled to the anti-virus application, said dat file updater and validater configured to periodically download updated virus data, validate the updated virus data after download, and update said anti-virus application with said updated virus data after validating said virus data. However Hodges et al (6, 269,456 B1) disclose a "dat file updater and validater" coupled to the anti-virus application, said dat file updater and validater configured to periodically download updated virus data, validate the updated virus data after download, and update said anti-virus application with said updated virus data after validating said virus data **(see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file**

and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application system in Chen's anti virus detection system where every incoming file is being scanned by check in inceptor **in order to provide the most up-to-date, or even up-to hour anti virus protection available.**

As per claim 14 Chen et al (5,832,208 A) teach all limitation of method of claim 10 as applied above but do not explicitly disclose:

a) periodically downloading updated virus data;

b) validating the updated virus data; and

c) updating said anti-virus application with said updated virus data.

However Hodges et al (6, 269,456 B1) disclose periodically downloading updated virus data; validating the updated virus data; and updating said anti-virus application with said updated virus data **(see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application method in

Chen's anti virus detection method where every incoming file is being scanned by check in inceptor **in order to provide the most up-to-date, or even up-to hour anti virus protection available.**

As per claim 20 Chen et al (5,832,208 A) teach all limitation of the program storage device of claim 16 as applied above but not explicitly disclose:

a) periodically downloading updated virus data;

b) validating the updated virus data; and

c) updating said anti-virus application with said updated virus data.

However Hodges et al (6, 269,456 B1) disclose the program storage device for downloading updated virus data according to a periodically downloading updated virus data; validating the updated virus data; and updating said anti-virus application with said updated virus data **(see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application virus detection program device for scanning incoming file by check in interceptor device **in order to provide the most up-to-date, or even up-to hour anti virus protection available.**

As per claim 26 Chen et al (5,832,208 A) Chen et al (5,832,208 A) teach the virus detection monitoring system of claim 22, further comprising:

a) means for downloading updated virus data according to a schedule;

b) means for validating the updated virus data; and

c) means for updating said anti-virus application with said updated virus data.

However Hodges et al (6, 269,456 B1) disclose means for downloading updated virus data according to a schedule; means for validating the updated virus data; and means for updating said anti-virus application with said updated virus data **(see col.7, lines 1-12 where the file virus_signature.dat that corresponds to Applicant's dat file updater and validater configured to periodically such as monthly, or weekly, daily or even hourly update the dat file and validate the new update by integrating the new signature into the file virus_signature.dat by anti virus application manufacturer)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hodges et al's automated updating and upgrading of antivirus application means in Chen's anti virus detection means where every incoming file is being scanned by check in inceptor means **in order to provide the most up-to-date, or even up-to hour anti virus protection available.**

11. **Claims 7, 15, 21 and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (5,832,208 A) in view of McGrane (6,760,760 B1).

As per claims 7, 15, 21 and 27 Chen et al (5,832,208 A) teach all limitation of the claims including agent 11 of fig.2 that also corresponds to the virus detection monitoring system of claims 1, 10, 16 and 22, but do not explicitly disclose said check-in interceptor inspects documents and files uploaded to an electronic document control system operating on the network server. However McGrane (6,760,760 B1) disclose uploaded of files to an electronic document control system operating on the network server **(see fig.2-4 where the control system operating under the network server transfer uploaded data to the server; col.2, lines 61-63; col.4, lines 6-17 where it disclose a bi-directional communication and that the uploading of files are being send to the server where uploading may be in any direction). It also discloses more than one link between the server and the controller)**. It would have been obvious to one of ordinary skilled in the art to link MacGrane's file controller system where the uploaded file is stored to Chen's agent 11 of figure 2 that corresponds to check in interceptor **in order to provide establish a pathway to one or more control systems to enable bi-directional transfer of uploaded data and files to be intercepted and scanned by Chen's anti virus interceptor agent**.

12. **Claims 8 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al (5,832,208 A) in view of Tso et al (6,088,803 A).

As per claims 8 and 9 Chen et al (5,832,208 A) teach all limitation of the claim as applied in claim 1 above but do not disclose the interception of files comprising of

uploaded commands and hypertext transfer protocol commands issued to the server. However Tso et al (6,088,803 A) disclose uploaded commands and hypertext transfer protocol commands issued to a server **(see fig.5, item 36; col.7, lines 13-23 where operation of read (uploading) and write (downloading) command for hypertext transfer protocol (http) is being processed where such file under that commands regardless of being uploaded or downloaded in any type of format such as html are subject to virus checker as disclosed on col.3, lines 2-4**). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Tso et al's uploaded and HTTP commands in Chen's et al's anti-virus scanning file system **in order to scan such internet downloaded/uploaded files for virus detection in order to prevent transmission of file and issuing an appropriate error warning message to client device or the server that holds the file.**

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (5,559,960 A) teach software anti-virus facility.

b. U.S.Patent No. US (5,978,917 A) teach detection and elimination of macro viruses.

c. U.S.Patent No. US (5,473,769 A) teach method and apparatus for increasing the speed of the detection of computer virus.

d. U.S.Patent No. US (5,485,575 A) teach automatic analysis of a computer virus structure and means of attachment to its hosts.

e. U.S.Patent No. US (5,613,002 A) teach generic disinfection of programs infected with a computer virus.

f. U.S.Patent No. US (5,696,822 A) teach polymorphic virus detection module.

g. U.S.Patent No. US (5,956,481 A) teach method and apparatus for protecting data files on a computer from virus infection.

U.S.Patent No. US (5,948,104 A) teach system and method for automated anti-viral file update.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see

http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

07/24/04